The number of cyclic configurations of type (v_3) and the isomorphism problem

S. Hiroki Koike-Quintanar *
IAM, University of Primorska
Muzejski trg 2, 6000 Koper, Slovenia
hiroki.koike@iam.upr.si

István Kovács †
IAM and FAMNIT, University of Primorska
Muzejski trg 2, 6000 Koper, Slovenia
istvan.kovacs@upr.si

Tomaž Pisanski ‡
FMF, University of Ljubljana
Jadranska 19, 1000 Ljubljana, Slovenia
Tomaz.Pisanski@fmf.uni-lj.si

January 14, 2013

Abstract

A configuration of points and lines is cyclic if it has an automorphism which permutes its points in a full cycle. A closed formula is derived for the number of non-isomorphic connected cyclic configurations of type (v_3), i.e., which have v points and lines, and each point/line is incident with exactly 3 lines/points. In addition, a Bays-Lambossy type theorem is proved for cyclic configurations if the number of points is a product of two primes or a prime power.

Keywords: cyclic configuration, cyclic object, isomorphism.

MSC 2010: 20B25, 51E30, 05C25, 05C60.

*Supported in part by ARRS - Agencija za raziskovanje Republike Slovenija, program no. P1-0285.

†Supported in part by ARRS - Agencija za raziskovanje Republike Slovenija, program no. P1-0285 and project N1-0011 (ESF EUROCORES EUROGiga/GReGAS)..

‡Supported in part by ARRS - Agencija za raziskovanje Republike Slovenija, program no. P1-0294 and project N1-0011 (ESF EUROCORES EUROGiga/GReGAS).

1 Introduction

An *incidence geometry* $(P, \mathcal{B})$ consists of a set of v points $P = \{p_1, ..., p_v\}$ and a collection of b lines (or blocks) $\mathcal{B} = \{B_1, ..., B_b\}$ such that $B_i \subseteq P$ for every $i \in \{1, ..., b\}$, and $|B_i \cap B_j| \leq 1$ for every $i, j \in \{1, ..., b\}$ and $i \neq j$. An incidence geometry is called a *configuration* of type (v_r, b_k) (*combinatorial configuration* in the sense of [6]) if

- $|\{B_j \in \mathcal{B} : p_i \in B_j\}| = r$ for every $i \in \{1, .., v\}$; and
- $|B_j| = k$ for every $j \in \{1, .., b\}$ with $k \geq 3$.

A configuration with $v = b$ (and therefore $r = k$) is called *balanced,* or a *k-configuration,* and its type is simply denoted by (v_k). A configuration $(P, \mathcal{B})$ is called *decomposable* if it is the disjoint union of two configurations $(P_r, \mathcal{B}_r), r = 1, 2$, i.e., $P = P_1 \cup P_2$, $P_1 \cap P_2 = \emptyset$, and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Indecomposable configurations are also called *connected*. An *isomorphism* between two incidence geometries $(P_r, \mathcal{B}_r), r = 1, 2$, is a bijective mapping $\sigma : P_1 \to P_2$ which maps $\mathcal{B}_1$ onto $\mathcal{B}_2$. Here a block $B \in \mathcal{B}_1$ with $B = \{p_1, ..., p_k\}$ is mapped onto $B^\sigma = \{p_1^\sigma, ..., p_k^\sigma\}$. If $(P_1, \mathcal{B}_1) = (P_2, \mathcal{B}_2)$, then σ is called an *automorphism*; the group of all automorphisms will be denoted by $\mathrm{Aut}((P_1, \mathcal{B}_1))$. An incidence geometry is *cyclic*, if it has an automorphism which permutes its points in a full cycle. In this case it is natural to identify the points with elements in the ring $\mathbb{Z}_v$, and assume that the translation $x \mapsto x + 1$ is an automorphism. Now, two incidence geometries are said to be *multiplier equivalent*, if there exits a unit $a \in \mathbb{Z}_n^*$ such that the mapping $x \mapsto ax$ induces an isomorphism between them.

The enumeration problem for configurations (both geometrical and combinatorial) attracted considerable attention (see the monograph [6, Chapters 2-3]). The list of all configurations of type (v_3) up to $v = 18$ was produced in [3], and for an approach based on the respective Levi graphs, we refer to [4, 16, 17]. The latter approach is based on the easy but crucial observation that combinatorial k-configurations are the same things as bipartite k-valent graphs with a given black-and-white coloring. In this paper we are going to calculate the number of cyclic configurations of type (v_3). For this purpose we set the notation $\#C(v_k)$ for the number of non-isomorphic coonected cyclic configurations of type (v_k). Our main result is the following closed formula for $\#C(v_3)$:

Theorem A. *Let $v > 4$ be an integer with prime factorization $v = p_1^{n_1} \cdots p_k^{n_k}$. Then*

$$\#C(v_3) = \begin{cases} \frac{v}{6} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right) + \alpha 2^k - 2 & \text{if } v \text{ is odd,} \\ \frac{v}{6} \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right) + \beta 2^k - 3 & \text{if } v \text{ is even,} \end{cases} \tag{1}$$

where α is defined for v odd by

$$\alpha = \begin{cases} 5/6 & \text{if every } p_i \equiv 1 (mod\ 3), \\ 2/3 & \text{if } p_1^{n_1} = 3 \text{ and if } i > 1, \text{ then } p_i \equiv 1 (mod\ 3), \\ 1/2 & \text{otherwise,} \end{cases}$$

and β is defined for v even by

$$\beta = \begin{cases} 1/4 & \text{if } v \equiv 2 (mod\ 8) \text{ or } v \equiv 6 (mod\ 8), \\ 1/2 & \text{if } v \equiv 4 (mod\ 8), \\ 1 & \text{if } v \equiv 0 (mod\ 8). \end{cases}$$

The crucial fact towards Theorem A is that the isomorphism problem in this case can be solved entirely by means of multiplier equivalence. More precisely, every two cyclic configurations of type (v_3) are isomorphic if and only if they are multiplier equivalent. This fact we are going to deduce as a direct consequence of a result about circulant matrices proved in [20]. It is interesting to note that this is no longer true for arbitrary cyclic configurations with 3 points on a line. In [19], Phelps gives examples of cyclic 2–$(v, 3, 1)$ designs which are isomorphic but not multiplier equivalent. In Section 2 we review the relevant results on circulant matrices and explain the relation with configurations. Section 3 is devoted to the proof of Theorem A.

In Section 4 we turn to the following question:

Question 1.1. *Given an integer v, is it true that any two balanced cyclic configurations on v points are isomorphic if and only if they are multiplier equivalent?*

This is part of the more general question which asks if a given finite group G has the *CI-property* for a given class $\mathcal{K}$ of relational structures on G (see [1, 15]). This question has been extensively studied under various choices of G and $\mathcal{K}$ (see, e.g. [8, 9, 11, 14, 19], just to mention those papers that will be invoked in the sequel). The finite groups having the CI-property for all relational structures (for short the CI-groups) were characterized by Pálfy in [15]. It turns out that these are the cyclic groups of order n with $n = 4$ or $\gcd(n, \phi(n)) = 1$ where ϕ denotes Euler's ϕ function. Consequently, Question 1.1 is answered in the positive if $v \geq 7$ and $\gcd(v, \phi(v)) = 1$. In Section 4 we provide further values of v inducing a positive answer by proving the following theorem:

Theorem B. *If $v = pq$ or $v = p^n$, p, q are primes, then any two balanced cyclic configurations on v points are isomorphic if and only if they are multiplier equivalent.*

Remark 1.2. Theorem B can be viewed as a Bays-Lambossy type theorem for balanced cyclic configurations. It was proved first by Bays in [2] and Lambossy in [13] that two cyclic Steiner triple systems on a prime number of points are isomorphic if and only if they are multiplier equivalent. It is worth noted that the Bays-Lambossy Theorem was generalized to abelian projective planes (see [11, Corollary 2.2]).

2 Circulant matrices

Lemma 2.1. *Let $\mathcal{C} = (\mathbb{Z}_v, \mathcal{B})$ be a balanced configuration with the translation $x \mapsto x+1$ in $\mathrm{Aut}(\mathcal{C})$. Then there exists a subset S of $\mathbb{Z}_v$ such that $\mathcal{B}$ consists of the sets in the form $S + i$, $i \in \mathbb{Z}_v$.*

PROOF: Denote by G the group generated by the translation $x \mapsto x+1$. Choose a line $B \in \mathcal{B}$ such that $0 \in B$, where 0 is the zero element of $\mathbb{Z}_v$. Assume for the moment that B satisfies

$$B^g = B \text{ or } B^g \cap B = \emptyset \text{ for every } g \in G. \tag{2}$$

In other words, B is a block for the permutation group G (see [5, page 12.]). This gives that B is an orbit of a subgroup of G of size k (see [5, Theorem 1.5A]), where k is the size of the lines. Since G is a cyclic group, the set B is uniquely determined. Choose next a line $B' \in \mathcal{B}$ for which $0 \in B'$ and $B' \neq B$. Then (2) does not hold for B', i.e., there exists $g \in G$ such that B' and B'^g intersects at a unique point, say i ($i \in \mathbb{Z}_v$).

Let us consider the action of G on the set $\mathcal{B}$. We denote by $G_{B'}$ the stabilizer of the line B' in this action, i.e., $G_{B'} = \{g \in G : B'^g = B'\}$. Then $G_{B'^g} = g^{-1}G_{B'}g$, $|G_{B'^g}| = |G_{B'}|$, and so $G_{B'^g} = G_{B'}$ (again, G is a cyclic group). Clearly, every element in $G_{B'} \cap G_{B'^g}$ fixes the point i. Since G is regular on the points, we obtain $G_{B'} = G_{B'} \cap G_{B'^g} = 1$. The orbit-stabilizer property (see [5, Theorem 1.4A]) gives that the orbit of B' under G is of length $|G| = |P| = |\mathcal{B}|$. Letting $S = B'$, the lemma follows. ∎

We shall refer to the set S in Lemma 6 as a *base line* of $\mathcal{C}$, and use the symbol $\mathrm{Con}(\mathbb{Z}_v, S)$ for $\mathcal{C}$. Base lines are characterized in the next lemma.

Lemma 2.2. [7] *The following (1)-(2) are equivalent for every subset S of $\mathbb{Z}_v$.*

(1) S is a base line of a cyclic configuration of type (v_k).

(2) $|S| = k$ and $|S - S| = k^2 - k + 1$.[1]

Suppose that S is a base line such that $0 \in S$ (clearly, every configuration admits base lines with this property). The set S generates a subgroup of $\mathbb{Z}_v$, say of order d, and denote it by $\mathbb{Z}_d$. Then $\mathrm{Con}(\mathbb{Z}_d, S)$ is a connected configuration. Also, $\mathrm{Con}(\mathbb{Z}_v, S)$ decomposes to the union of v/d copies of $\mathrm{Con}(\mathbb{Z}_d, S)$:

$$\mathrm{Con}(\mathbb{Z}_v, S) \cong \mathrm{Con}(\mathbb{Z}_d, S) \cup \cdots \cup \mathrm{Con}(\mathbb{Z}_d, S). \tag{3}$$

Note that, if S is an arbitrary base line (0 is not necessarily in S), then it holds:

$$\mathrm{Con}(\mathbb{Z}_v, S) \text{ is connected } \iff \langle S - S \rangle = \mathbb{Z}_v. \tag{4}$$

The following necessary condition for a set to be a base line will be used frequently through the paper. It follows promptly from the second part in (2) of Lemma 2.2.

Corollary 2.3. *If a subset S of $\mathbb{Z}_v$ is a base line of a cyclic configuration, then S contains no H-coset for every nontrivial subgroup $H \leq \mathbb{Z}_v$.*

For positive integers v and k denote by $B(v,k)$ the set of all base lines of $\mathbb{Z}_v$ of size k, and by $B_{\mathrm{con}}(v,k)$ the set of those which define connected configurations. More formally,

$$\begin{aligned} B(v,k) &= \{X \subseteq \mathbb{Z}_v : |X| = k \text{ and } |X - X| = k^2 - k + 1\}, \\ B_{\mathrm{con}}(v,k) &= \{X \in B(v,k) : \langle X - X \rangle = \mathbb{Z}_v\}. \end{aligned}$$

[1] Here $S - S = \{s_1 - s_2 : s_1, s_2 \in S\}$.

Notice that, if $X \in B(v,k)$, $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$, then the set $aX+b$ is also in $B(v,k)$. Hence the mapping $X \mapsto aX+b$ defines an action of the *affine group* $AGL_1(v)$ on $B(v,k)$. Clearly, the subset $B_{\mathrm{con}}(v,k)$ of $B(v,k)$ is invariant with respect to this action.

Next, we review the definition of a circulant matrix. Let A be an v-by-v matrix. The matrix A is a *permutation matrix* if it is a $(0,1)$ matrix, and every row and column contains exactly one 1's. Furthermore, $A=(a_{i,j})$ is a *circulant matrix* if $a_{i+1,j+1}=a_{i,j}$ holds for every $i,j \in \{0,1,...,v-1\}$, where the additions in subscripts are modulo v. Here we label rows and columns by elements of $\mathbb{Z}_v$. We let $\mathbb{Z}_v=\{0,1,...,v-1\}$, the leftmost column is labeled 0, the next is 1 and so on. If $A=(a_{i,j})$ is an v-by-v $(0,1)$ circulant matrix, then denote by S_A the subset of $\mathbb{Z}_v$ defined by

$$S_A=\{i \in \mathbb{Z}_v : a_{0,\,i}=1\}.$$

The cardinality $|S_A|$ is also called the *weight* of A. Also, A^T denotes the transpose of the matrix A.

Let $S \in B(v,k)$, and let A be the $(0,1)$ circulant matrix defined by $S_A=S$. Then it follows immediately from the definitions that, A is a *line-point incidence matrix* of the cyclic configuration $\mathrm{Con}(\mathbb{Z}_v,S)$ (see [6]).

Lemma 2.4. *For $r=1,2$, let $S_r \in B(v,k)$, and let A_r be the $(0,1)$ circulant matrix defined by $S_{A_r}=S_r$. The following equivalence holds:*

$$\mathrm{Con}(\mathbb{Z}_v,S_1) \cong \mathrm{Con}(\mathbb{Z}_v,S_2) \iff A_1=PA_2Q$$

for some v-by-v permutation matrices P and Q.

Proof: Let P and Q arbitrary v-by-v permutation matrices. Associate then the permutation π of $\mathbb{Z}_v$ with P and the permutation σ of $\mathbb{Z}_v$ with Q as follows:

$$i^\pi=j \overset{def}{\iff} P_{i,j}=1 \text{ and } i^\sigma=j \overset{def}{\iff} Q_{j,i}=1 \text{ for evey } i,j \in \mathbb{Z}_v.$$

Then

$$(PA_2Q)_{i,j}=\sum_{k,l=0}^{v-1} P_{i,k}(A_2)_{k,l}Q_{l,j}=(A_2)_{i^\pi,j^\sigma}.$$

Now, $A_1=PA_2Q$ can be interpreted as the permutation σ maps the line S_1+i to the line S_2+i^π. Equivalently, σ induces an isomorphism from $\mathrm{Con}(\mathbb{Z}_v,S_1)$ to $\mathrm{Con}(\mathbb{Z}_v,S_2)$. The lemma follows. ∎

Lemma 2.4 brings us to the following result of Wiedman and Zieve:

Theorem 2.5. [20, Theorem 1.1] *The following (1)-(4) are equivalent for every two v-by-v $(0,1)$ circulant matrices A_1 and A_2 of weight at most 3.*

(1) There is $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$ such that $S_{A_1}=aS_{A_2}+b$.

(2) There are v-by-v permutation matrices P,Q such that $A_1=PA_2Q$.

(3) There is an v-by-v permutation matrix P such that $A_1A_1^T = PA_2A_2^TP^{-1}$.

(4) The complex matrices $A_1A_1^T$ and $A_2A_2^T$ are similar.

Notice that, the configurations $\mathrm{Con}(\mathbb{Z}_v, S_1)$ and $\mathrm{Con}(\mathbb{Z}_v, S_2)$ are multiplier equivalent if and only if $S_1 = aS_2 + b$ for some $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$. Combining this with Lemma 2.4 and Theorem 2.5, we obtain the required equivalence for configurations of type (v_3):

Corollary 2.6. *Any two cyclic configurations of type (v_3) are isomorphic if and only if these are multiplier equivalent.*

As pointed out in [20], the equivalences in Theorem 2.5 do not hold when the weight $k \geq 4$. The following theorem settles the case $k = 4$. It is was proved by the first two authors in the context of cyclic Haar graphs (see [12, Theorem 1.1]), below it is rephrased in terms of circulant matrices.

Theorem 2.7. *The following (1)-(2) are equivalent for two v-by-v $(0,1)$ circulant matrices A_1 and A_2 of weight 4 such that $\langle S_{A_r} - S_{A_r}\rangle = \mathbb{Z}_v$ for both $r = 1, 2$.*

(1) There exist $a_1, a_2 \in \mathbb{Z}_v^*$ and $b_1, b_2 \in \mathbb{Z}_v$ such that

(1a) $S_{A_1} = a_1S_{A_2} + b_1$; or

(1b) $a_1S_{A_1} + b_1 = \{0, x, y, y+u\}$ and $a_2S_{A_2} + b_2 = \{0, x+u, y, y+u\}$, where $v = 2u$, $\mathbb{Z}_v = \langle x, y\rangle$, $2 \mid x$, $(2x) \mid u$ and $x/2 \not\equiv y + u/(2x) (mod\ u/x)$.

(2) There are v-by-v permutation matrices P, Q such that $A_1 = PA_2Q$.

Corollary 2.8. *Any two cyclic configurations of type (v_4) are isomorphic if and only if these are multiplier equivalent.*

Proof: We prove the statement for connected configurations. The general case follows then by using the decomposition in (3) and induction on v.

Let $\mathrm{Con}(\mathbb{Z}_v, S_r)$, $r = 1, 2$, be two connected configurations of type (v_4). Then $\langle S_r - S_r\rangle = \mathbb{Z}_v$, see (4), and we apply Theorem 2.7 to the respective line-point incidence matrices. Now, one only needs to exclude the possibility that the sets S_r are described by part (1b) of Theorem 2.7. That this is indeed the case follows from Corollary 2.3 where choose H to be the subgroup of order 2. ∎

Remark 2.9. As noted in the introduction, cyclic configurations are equivalent to cyclic Haar graphs of girth 6, and therefore each of our results has a counterpart in the context of cyclic Haar graphs. In this spirit [18, Theorem 5.23] summarizes Corollaries 2.6 and 2.8.

3 Proof of Theorem A

Recall that, two configurations $\mathrm{Con}(\mathbb{Z}_v, S_r)$, $r = 1, 2$, are multiplier equivalent if and only if their base lines S_r are in the same orbit of $AGL_1(v)$. Thus Corollary 2.6 gives that $\#C(v_3)$ is equal to the number of orbits of $AGL_1(v)$ acting on $B_{\mathrm{con}}(v, 3)$.

Lemma 3.1. *Let v and k be integers such that $k \geq 3$ and $v \geq k^2 - k + 1$, and denote by $\mathcal{N}$ the number of orbits of $AGL_1(v)$ acting on $B_{\mathrm{con}}(v, k)$. Then*

$$\mathcal{N} = \frac{1}{k\phi(v)} \sum_{l \in \mathbb{Z}_v^*} N(v, k, l),$$

where $N(v, k, l) = \big\{X \in B_{\mathrm{con}}(v, k) : 0 \in X$ and $lX = X - x$ for some $x \in X\big\}$.

Proof: For short we put $B_0 = \{X \in B_{\mathrm{con}}(v, k) : 0 \in X\}$, and for $X \in B_0$ with $X = \{x_1, x_2, ..., x_k\}$, define the set

$$\widehat{X} = \{X - x_1, X - x_2, ..., X - x_k\}.$$

It is easily seen that for every set $Y = X - x_i$ it holds $\widehat{Y} = \widehat{X}$. It follows from this that the sets $\widehat{X}, X \in B_0$, form a partition of B_0. This partition will be denoted by π. Notice also that $|\widehat{X}| = k$ holds for every class $\widehat{X} \in \pi$ because $|X - X| = k^2 - k + 1$ (see (2) in Lemma 2.2). Let us consider the action of $\mathbb{Z}_v^*$ on B_0 defined by $X^l = l\,X = \{lx : x \in X\}$ for every $l \in \mathbb{Z}_v^*$ and $X \in B_0$. The partition π is preserved by $\mathbb{Z}_v^*$ in this action, denote by $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ the set of the corresponding orbits. For $X \in B_0$, denote by $O(X)$ the orbit of X under $AGL_1(v)$, and by $O(\widehat{X})$ the orbit of $\widehat{X}$ under $\mathbb{Z}_v^*$.

We claim that the mapping $f : O(\widehat{X}) \mapsto O(X)$ establishes a bijection from $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ to the set of orbits of $AGL_1(v)$ acting on $B_{\mathrm{con}}(v, k)$ (notice that, the mapping f is well-defined). It is clear that f is surjective. To settle that it is also injective choose $X, Y \in B_{\mathrm{con}}(v, k)$ such that $O(X) = O(Y)$. We may assume without loss of generality that $0 \in X \cap Y$. By definition, $Y = aX + b$ for some $a \in \mathbb{Z}_v^*$ and $b \in \mathbb{Z}_v$. Since $0 \in Y$, $b = -ax$ for some $x \in X$. Thus $a'Y = X - x$, where $aa' \equiv 1 (\mathrm{mod}\ v)$, implying that $O(\widehat{X}) = O(\widehat{Y})$, and so f is also injective, hence bijective. We obtain that the required number $\mathcal{N} = |\,\mathrm{Orb}(\mathbb{Z}_v^*, \pi)|$. Then the orbit-counting lemma applied to $\mathrm{Orb}(\mathbb{Z}_v^*, \pi)$ yields the formula (see [5, Theorem 1.7A]):

$$\mathcal{N} = \frac{1}{\phi(v)} \sum_{l \in \mathbb{Z}_v^*} \big|\{\widehat{X} \in \pi : \widehat{X}l = \widehat{X}\}\big|.$$

In order to finish the proof one only needs to observe that $\widehat{X}l = \widehat{X}$ happens exactly when $lX = X - x$ for some $x \in X$; and if this is so, then every set $Y \in \widehat{X}$ satisfies $lY = Y - y$ for some $y \in Y$. This gives us

$$|\{\widehat{X} \in \pi : \widehat{X}l = \widehat{X}\}| = \frac{N(v, k, l)}{k}.$$

The lemma is proved. ∎

By Corollary 2.6 and Lemma 3.1, we find that,

$$\#C(v_3) = \frac{1}{3\phi(v)} \sum_{l \in \mathbb{Z}_v^*} N(v,3,l). \tag{5}$$

We compute next the parameters $N(v,3,l)$ in (5).

Define first the function $\Phi : \mathbb{N} \to \mathbb{N}$ by $\Phi(1) = 1$, and for $v > 1$ let

$$\Phi(v) = v\Big(1 + \frac{1}{p_1}\Big) \cdots \Big(1 + \frac{1}{p_k}\Big),$$

where v has prime factorization $v = p_1^{n_1} \cdots p_k^{n_k}$. Obviously, Φ is a multiplicative function, i.e., $\Phi(v_1 v_2) = \Phi(v_1)\Phi(v_2)$ whenever $\gcd(v_1, v_2) = 1$.

Lemma 3.2. *If $v > 4$, then*

$$N(v,3,1) = \begin{cases} \frac{1}{2}\phi(v)(\Phi(v) - 6) & \text{if } v \text{ is odd,} \\ \frac{1}{2}\phi(v)(\Phi(v) - 6) - 3\phi(v/2) & \text{if } v \text{ is even.} \end{cases}$$

Proof: Define the sets:

$$\begin{aligned} S(v) &= \{(x,y) \in \mathbb{Z}_v \times \mathbb{Z}_v : \langle x, y\rangle = \mathbb{Z}_v\}, \\ S^*(v) &= \{(x,y) \in S(v) : |\{0, x, y, -x, -y, x-y, y-x\}| < 7\}. \end{aligned}$$

We leave for the reader to verify that the function $v \mapsto |S(v)|$ is multiplicative. Let $v = p^n$, p is a prime. Then two elements x, y generate $\mathbb{Z}_v$ if and only if one of them is a generator. By this we calculate that $|S(v)| = 2\phi(v)v - \phi(v)^2 = \phi(v)(2v - \phi(v)) = \phi(v)\,\Phi(v)$. We find, using that all functions ϕ, Φ and $v \mapsto |S(v)|$ are multiplicative, that $|S(v)| = \phi(v)\,\Phi(v)$ for every number v.

Now, for every $x, y \in \mathbb{Z}_v$, $\{0, x, y\} \in B_{\mathrm{con}}(v,3)$ if and only if $(x,y) \in S(v) \setminus S^*(v)$. Therefore,

$$N(v,3,1) = \frac{|S(v)| - |S^*(v)|}{2} = \frac{1}{2}\big(\,\phi(v)\Phi(v) - |S^*(v)|\,\big). \tag{6}$$

It remains to calculate $|S^*(v)|$. Let v be odd. Then $S^*(v)$ can be expressed as

$$S^*(v) = \{(0,x), (x,0), (x,x), (x,-x), (x,2x), (2x,x) : x \in \mathbb{Z}_v^*\}.$$

Since $v > 4$, there is no coincidence between the above pairs, and so $|S^*(v)| = 6\phi(v)$. The formula for $N(v,3,1)$ follows by this and (6).

Let v be even, say $v = 2u$. In this case

$$\begin{aligned} S^*(v) &= \{(0,x), (x,0), (x,x), (x,-x), (x,2x), (2x,x) : x \in \mathbb{Z}_v^*\} \cup \\ &\quad \{(u,x), (x,u), (x,x+u) : x \in \mathbb{Z}_v \text{ and } \langle x, u\rangle = \mathbb{Z}_v\}. \end{aligned}$$

Again, since $v > 4$, there is no coincidence between the above pairs. A quick computation gives that $|S^*(v)| = 6\phi(v) + 6\phi(u)$. The formula for $N(v, 3, 1)$ follows by this and (6). The lemma is proved. ∎

For $l \in \mathbb{Z}_v^*$, denote by $\mathrm{ord_m}(l)$ the order of l as an element of $\mathbb{Z}_v^*$. Furthermore, $O(l)$ denotes the set of orbits of $\mathbb{Z}_v$ under l, i.e.,

$$O(l) = \left\{ \{x, lx, ..., l^{m-1}x\} : x \in \mathbb{Z}_v \right\} \text{ where } m = \mathrm{ord_m}(l).$$

Lemma 3.3. *Let $l \in \mathbb{Z}_v^*$, $l \neq 1$.*

(i) If $\mathrm{ord_m}(l) > 3$, then $N(v, 3, l) = 0$.

(ii) If $\mathrm{ord_m}(l) = 2$, then

$$N(v,3,l) = \begin{cases} 0 & \text{if } l+1 \equiv 0 (mod\ v),\ \text{or } v \equiv 0 (mod\ 4) \text{ and } l \equiv 1 (mod\ v/2), \\ \frac{3\phi(v)}{2} & \text{otherwise.} \end{cases}$$

(iii) If $\mathrm{ord_m}(l) = 3$, then

$$N(v,3,l) = \begin{cases} 0 & \text{if } l^2 + l + 1 \not\equiv 0 (mod\ v), \\ \phi(v) & \text{otherwise.} \end{cases}$$

Proof: Put again $B_0 = \{X \in B_{\mathrm{con}}(v, 3) : 0 \in X\}$, and let $X \in B_0$ such that $X = \{0, x, y\}$ and

$$lX = X \text{ or } lX = X - x. \tag{7}$$

We consider step-by-step all cases (i)-(iii).

(i): Assume by contradiction that (7) holds for some $l \in \mathbb{Z}_v^*$ with $\mathrm{ord_m}(l) > 3$. If $Xl = X$, then $l^2x = x$ and $l^2y = y$. This together with $\langle x, y\rangle = \mathbb{Z}_v$ imply that $l^2 \equiv 1 (\mathrm{mod}\ v)$, a contradiction to $\mathrm{ord_m}(l) > 2$. Let $Xl = X - x$, and so $\{lx, ly\} = \{-x, y - x\}$. Now, if $lx = -x$ and $ly = y - x$, then $l^2x = x$ and $l^2y = y$ which is impossible. If $lx = y - x$ and $ly = -x$, then $l^3x = x$ and $l^3y = y$, implying that $l^3 \equiv 1 (\mathrm{mod}\ v)$, which is in contradiction with $\mathrm{ord_m}(l) > 3$.

(ii): Assume that (7) holds with $\mathrm{ord_m}(l) = 2$. If $lX = X$, then $lx = y$ and $ly = x$ and so we find X as $X = \{0, x, lx\}$, $x \in \mathbb{Z}_v^*$. Let $lX = X - x$. Then it follows that $lx = -x$ and $ly = y - x$ (otherwise $l^3 \equiv 1 (\mathrm{mod}\ v)$, a contradiction to $\mathrm{ord_m}(l) = 2$), and so $X = \{0, y, -ly + y\}$ where $y \in \mathbb{Z}_v^*$. Since $X \in B_0$, the elements $0, 1, -1, l, -l, l - 1$ and $1 - l$ must be pairwise distinct. We conclude from these that, $N(v, 3, l) = 0$ if $l+1 = 0 (\mathrm{mod}\ v)$ or $l \equiv 1 (\mathrm{mod}\ v/2)$, and otherwise $N(v, 3, l)$ is the size of the following set:

$$\left\{\{0, x, lx\} : x \in \mathbb{Z}_v^*\right\} \cup \left\{\{0, x, -lx + x\} : x \in \mathbb{Z}_v^*\right\}.$$

We observe in turn that, the two sets above are disjoint, the first has size $\phi(v)/2$, while the second has cardinality $\phi(v)$. Then (ii) follows.

(iii): Assume that (7) holds with $\mathrm{ord}_{\mathrm{m}}(l) = 3$. Then $X = lX - x$, $lx = y - x$ and $ly = -x$ (otherwise $l^2 \equiv 1 (\mathrm{mod}\ v)$, see above). Thus $X = \{0, x, x + lx\}$, $x \in \mathbb{Z}_v^*$ and $l^2 + l \equiv -1 (\mathrm{mod}\ v)$. We conclude that, $N(v, 3, l) = 0$ if $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$, and otherwise $N(v, 3, l) = \left|\left\{\{0, x, lx + x\} : x \in \mathbb{Z}_v^*\right\}\right| = \phi(v)$. Thus (iii) follows, and this completes the proof of the lemma. ∎

Proof of Theorem A: By Lemmas 3.1 and 3.2, the sum in (5) reduces to

$$\#C(v_3) = \begin{cases} \frac{1}{6}\Phi(v) - 1 + \frac{1}{2}\gamma_1 + \frac{1}{3}\gamma_2 & \text{if } v \text{ is odd,} \\ \frac{1}{6}\Phi(v) - \frac{\phi(v/2)}{\phi(v)} - 1 + \frac{1}{2}\gamma_1 + \frac{1}{3}\gamma_2 & \text{if } v \text{ is even,} \end{cases} \tag{8}$$

where γ_1 and γ_2 are defined by

$$\begin{aligned} \gamma_1 &= |\{l \in \mathbb{Z}_v^* : \mathrm{ord}_{\mathrm{m}}(l) = 2,\ l + 1 \not\equiv 0 (\mathrm{mod}\ v) \text{ and } l \not\equiv 1 (\mathrm{mod}\ v/2) \text{ if } v \equiv 0 (\mathrm{mod}\ 4)\}|, \\ \gamma_2 &= |\{l \in \mathbb{Z}_v^* : \mathrm{ord}_{\mathrm{m}}(l) = 3 \text{ and } l^2 + l + 1 \equiv 0 (\mathrm{mod}\ v)\}|. \end{aligned}$$

In calculating γ_1 and γ_2 below we shall use the fact $\mathbb{Z}_v^*$ can be written as $\mathbb{Z}_v^* = \mathbb{Z}_{p_1^{n_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{n_k}}^*$, and every $l \in \mathbb{Z}_v^*$ can be expressed as

$$l = (l_1, ..., l_k), \text{ where } l_i \in \mathbb{Z}_{p_i^{n_i}}^* \text{ for every } i \in \{1, ..., k\}. \tag{9}$$

Note that, we may assume that $l_i \equiv l (\mathrm{mod}\ p_i^{n_i})$ for every $i \in \{1, ..., k\}$.

Case 1. v is odd.

Since v is odd, there are exactly $2^k - 1$ elements $l \in \mathbb{Z}_v^*$ such that $\mathrm{ord}_{\mathrm{m}}(l) = 2$, and all but one contributes to γ_1 (namely, $l = v - 1$ is excluded in the definition of γ_1). Thus $\gamma_1 = 2^k - 2$. The value of γ_2 depends solely on the residue of v modulo 9 and the reside of prime factors p_i modulo 3. Let $l \in \mathbb{Z}_v^*$ such that $\mathrm{ord}_{\mathrm{m}}(l) = 3$ and write $l = (l_1, ..., l_k)$ as described in (9). Thus l_i is of order 1 or 3 in $\mathbb{Z}_{p_i^{n_i}}^*$.

Case 1.1. $p_i \equiv 1 (\mathrm{mod}\ 3)$ for every $i \in \{1, ..., k\}$.

If l_i is of order 1 in $\mathbb{Z}_{p_i^{n_i}}^*$, then $l \equiv l_i \equiv 1 (\mathrm{mod}\ p_i^{n_i})$, from which $l^2 + l + 1 \equiv 3 (\mathrm{mod}\ p_i^{n_i})$, hence $l^2 + l + 1 \not\equiv 0 (\mathrm{mod}\ v)$, so l cannot contribute to γ_2. If l_i is of order 3 in $\mathbb{Z}_{p_i^{n_i}}^*$, then $l^2 + l + 1 \equiv l_i^2 + l_i + 1 \equiv 0 (\mathrm{mod}\ p_i^{n_i})$ for every $i \in \{1, ..., k\}$, hence $l^2 + l + 1 \equiv 0 (\mathrm{mod}\ v)$. Since there are exactly two elements in $\mathbb{Z}_{p_i^{n_i}}$ of order 3, $\gamma_2 = 2^k$. Substitute this and $\gamma_1 = 2^k - 2$ in (8). We obtain that $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{5}{6}2^k - 2$.

Case 1.2. $v \equiv 3 (\mathrm{mod}\ 9)$ and $p_i \equiv 0/1 (\mathrm{mod}\ 3)$ for every $i \in \{1, ..., k\}$.

We may write $p_1^{n_1} = 3$. We obtain, by the same argument as in the previous case, that l contributes to γ_2 if and only if l_1 is of order 1 in $\mathbb{Z}_{p_1^{n_1}}$, and l_i is of order 3 in $\mathbb{Z}_{p_i^{n_i}}^*$ if $i \geq 2$. Thus $\gamma_2 = 2^{k-1}$, which together with $\gamma_1 = 2^k - 2$ yield in (8) that $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{2}{3}2^k - 2$.

CASE 1.3. $v \equiv 0(\text{mod } 9)$ or $p_i \equiv 2(\text{mod } 3)$ for some $i \in \{1, ..., k\}$.

We show that in this case $l^2 + l + 1 \not\equiv 0(\text{mod } v)$ independently of the choice l. Thus $\gamma_2 = 0$, and so $\#C(v_3) = \frac{1}{6}\Phi(v) + \frac{1}{2}2^k - 2$.

Suppose first that $v \equiv 0(\text{mod } 9)$. We may write $p_1 = 3$, now $n_1 \geq 2$. Since $\text{ord}_{\text{m}}(l) = 3$, $l_1 \equiv 1(\text{mod } 3^{n_1-1})$. We claim that $l_1^2 + l_1 + 1 \equiv 3(\text{mod } 3^{n_1})$. Indeed, $l_1 \equiv 3^{n_1-1}k + 1(\text{mod } 3^{n_1})$ for some $k \in \{0, 1, 2\}$. Hence

$$l_1^2 + l_1 + 1 \equiv (k + 2k)3^{n_1-1} + 3 \equiv 3(\text{mod } 3^{n_1}).$$

Therefore, $l^2 + l + 1 \equiv l_1^2 + l_1 + 1 \equiv 3(\text{mod } 3^{n_1})$, and since $n_1 \geq 2$, $l^2 + l + 1 \not\equiv 0(\text{mod } 3_1^{n_1})$, and so $l^2 + l + 1 \not\equiv 0(\text{mod } v)$.

Suppose next that $p_i \equiv 2(\text{mod } 3)$ for some $i \in \{1, ..., k\}$. Then l_i must be of order 1 in $\mathbb{Z}_{p_i^{n_i}}$, and hence $l^2 + l + 1 \equiv l_i^2 + l_i + 1 \equiv 3(\text{mod } p_i^{n_i})$, and so $l^2 + l + 1 \not\equiv 0(\text{mod } v)$.

CASE 2. v is even.

Since v is even, l is odd, and thus $l^2 + l + 1 \not\equiv 0(\text{mod } v)$. We obtain that $\gamma_2 = 0$. The value of γ_1 depends on the residue of n modulo 8. The number of elements of order 2 in $\mathbb{Z}_v^*$ is $2^{k-1} - 1$ if $v \equiv 2/6(\text{mod } 8)$, $2^k - 1$ if $v \equiv 4(\text{mod } 8)$, and $2^{k+1} - 1$ if $v \equiv 0(\text{mod } 8)$ (see [10, Exercise 6.12]). Thus

$$\gamma_1 = \begin{cases} 2^{k-1} - 2 & \text{if} \quad v \equiv 2/6(\text{mod } 8), \\ 2^k - 3 & \text{if} \quad v \equiv 4(\text{mod } 8), \\ 2^{k+1} - 3 & \text{if} \quad v \equiv 0(\text{mod } 8). \end{cases} \tag{10}$$

Obviously, $\phi(v/2)/\phi(v) = 1$ if $v \equiv 2(\text{mod } 4)$ and it is $1/2$ if $v \equiv 0(\text{mod } 4)$. Substituting this, (10) and $\gamma_2 = 0$ in (8) yields formula (1). The theorem is proved. ∎

4 Proof of Theorem B

We consider cyclic configurations in the wider context of cyclic objects, where by a *cyclic object* of order v we mean a relational structure on $\mathbb{Z}_v$ which is invariant under the translation $\tau : x \mapsto x + 1$. The set of all cyclic objects of order v will be denoted by $\text{Obj}(\tau, \mathbb{Z}_v)$ (see [14]). An *isomorphism* between two cyclic objects $X_r, r = 1, 2$, is a permutation σ of $\mathbb{Z}_v$ which maps X_1 onto X_2, if $X = X_1 = X_2$, then σ is an *automorphism*, the group of all automorphisms will be denoted by $\text{Aut}(X)$. Given a class $\mathcal{K}$ of objects in $\text{Obj}(\tau, \mathbb{Z}_v)$, a *solving set* for $\mathcal{K}$ is a set Δ of permutations of $\mathbb{Z}_v$ satisfying the following property (see [14]):

$$(\forall X \in \mathcal{K})\ (\forall Y \in \text{Obj}(\tau, \mathbb{Z}_v))\ (X \cong Y \iff X^\sigma = Y \text{ for some } \sigma \in \Delta).$$

Pálfy's characterization of CI-groups (see the paragraph before Theorem B) yields the following theorem:

Theorem 4.1. [15] *The set $\mathbb{Z}_v^*$ is a solving set for* $\mathrm{Obj}(\tau, \mathbb{Z}_v)$ *if and only if* $v = 4$ *or* $\gcd(v, \phi(v)) = 1$.[2]

Let p and q be distinct primes. For every object $X \in \mathrm{Obj}(\tau, \mathbb{Z}_{pq})$, a solving set for X was determined by Huffman [8]. Before stating the relevant results, let us recall the required notations. For $j \in \mathbb{Z}_v^*$, let μ_j be the permutation $\mu_j : x \mapsto jx$. For $i \in \{0, 1, ..., q-1\}$, define the permutation τ_i by

$$\tau_i : x \mapsto \begin{cases} x+q & \text{if } x \equiv i(\mathrm{mod}\ q), \\ x & \text{otherwise,} \end{cases}$$

and if in addition $j \in \mathbb{Z}_v^*$ with $j \equiv 1(\mathrm{mod}\ q)$, then define the permutation $\mu_{i,j}$ by

$$\mu_{i,j} : x \mapsto \begin{cases} jx & \text{if } x \equiv i(\mathrm{mod}\ q), \\ x & \text{otherwise.} \end{cases}$$

For the next two theorems suppose in addition that q divides $p-1$. Furthermore, fix an element $a \in \mathbb{Z}_v^*$ of order $\mathrm{ord_m}(a) = p-1$ for which $a \equiv 1(\mathrm{mod}\ q)$, and put $b = a^{(p-1)/q}$.

Theorem 4.2. [8, Theorem 1.1] *Let $v = pq$, where p, q are primes such that q divides $p-1$, and let $X \in \mathrm{Obj}(\tau, \mathbb{Z}_v)$ such that $\mu_b \notin \mathrm{Aut}(X)$, where b is defined above. Then $\mathbb{Z}_v^*$ is a solving set for X.*

The powers $a, a^2, .., a^p$ are pairwise distinct modulo p. Let α be the positive integer in $\{1, 2, ..., p\}$ that $a^\alpha \equiv -s(\mathrm{mod}\ p)$, where $s = (p-1)/q$. For $i \in \{0, 1, ..., q-1\}$ define $\nu_i = \prod_{j=0}^{q-1} \mu_{j, a^\alpha b^{-ij}}$. Notice that, $\nu_0 = \mu_{a^\alpha}$. The next theorem is [8, Theorem 1.2], which, for our convenience, is formulated slightly differently.

Theorem 4.3. *Let $v = pq$, where p, q are primes such that q divides $p-1$, and let $X \in \mathrm{Obj}(\tau, \mathbb{Z}_v)$ such that $\mu_b \in \mathrm{Aut}(X)$ and $\tau_0 \notin \mathrm{Aut}(X)$, where b is defined above. Let β be the smallest positive integer such that $\mu_a^\beta \in \mathrm{Aut}(X)$. Then X admits a solving set Δ in the form:*

$$\Delta = \Big\{ \mu_a^i \, \nu_k \, \mu_j^{-1} : 0 \le i < \beta,\ 0 < j \le q-1,\ 0 \le k \le q-1,\ \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}} \in \mathrm{Aut}(X) \Big\}. \quad (11)$$

The last result before we prove Theorem B is a special case of [1, Lemma 3.1].

Lemma 4.4. *The following (1)-(2) are equivalent for every object $X \in \mathrm{Obj}(\tau, \mathbb{Z}_v)$.*

(1) $\mathbb{Z}_v^*$ is a solving set for X.

(2) Every two regular cyclic subgroup of $\mathrm{Aut}(X)$ *are conjugate in* $\mathrm{Aut}(X)$.

[2]Here $\mathbb{Z}_v^*$ denotes the set of permutations $x \mapsto ax$ where a goes over the set of all units in $\mathbb{Z}_v$.

PROOF OF THEOREM B: Obviously, the theorem can be rephrased as follows: $\mathbb{Z}_v^*$ is a solving set for the class of cyclic configurations on v points if $v = pq$ or $v = p^n$, where p, q are primes.

THE CASE $v = pq$: We prove the above statement for connected configurations. The general case follows then by using the decomposition in (3) and the fact that the statement is true for configurations with a prime number of points, so let $\mathcal{C} = \mathrm{Con}(\mathbb{Z}_{pq}, S)$ be a connected cyclic configuration.

Towards a contradiction assume that $\mathbb{Z}_{pq}^*$ is not a solving set for $\mathcal{C}$. Because of Theorem 4.1 we may also assume that q divides $p-1$. In the rest of the proof we keep the previous notations: τ_0, a, b, α and $\nu_0, \nu_1, ..., \nu_{q-1}$. Let $P = \{0, q, ..., (p-1)q\}$, i.e., the subgroup of $\mathbb{Z}_{pq}$ of order p. Replace S with a suitable line $S + i$ if necessary to ensure that $S \cap P \neq \emptyset$. Also, $S \not\subseteq P$ by the connectedness of X, i.e., there exists $t \in \{1, ..., q-1\}$ such that

$$S \cap P \neq \emptyset \text{ and } S \cap (P + t) \neq \emptyset. \tag{12}$$

Suppose for the moment that $\tau_0 \in \mathrm{Aut}(\mathcal{C})$. Using that τ_0 fixes every point outside P, (12) and that $|S| \geq 3$, we conclude $|S^{\tau_0^k} \cap S| \geq 2$ for some $k \in \{1, ..., q-1\}$. Hence $S^{\tau_0^k} = S$. As P is an orbit of τ_0^k, $P \subseteq S$, which contradicts Corollary 2.3. Thus $\tau_0 \notin \mathrm{Aut}(\mathcal{C})$.

Therefore, Theorems 4.2 and 4.3, together with the assumption that $\mathbb{Z}_{pq}^*$ is not a solving set, imply that $\mathcal{C}$ admits a solving set Δ defined in (11). Consider the permutation $\sigma = \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}}$, $k \in \{0, 1, ..., q-1\}$. If $k = 0$, then $\sigma = \tau^q$ which is clearly in $\mathrm{Aut}(\mathcal{C})$. The corresponding permutations in Δ are $\mu_a^i \, \nu_0 \, \mu_j^{-1} = \mu_a^i \, \mu_{a^\alpha} \, \mu_j^{-1}$. Since $\Delta \not\subseteq \mathbb{Z}_v^*$, there must exist $k > 0$ for which $\sigma = \prod_{l=0}^{q-1} \tau_l^{b^{(l+1)k}}$ belongs to $\mathrm{Aut}(\mathcal{C})$. Notice that,

$$\forall i, j \in \{0, 1, ..., q-1\} : \; i \neq j \implies b^{ik} \not\equiv b^{jk} (\mathrm{mod}\ p). \tag{13}$$

For otherwise, $b^{(i-j)k} \equiv 1 (\mathrm{mod}\ p)$. Since $\mathrm{ord}_{\mathrm{m}}(a) = p-1$, $a \equiv 1 (\mathrm{mod}\ q)$ and $b = a^{(p-1)/q}$, we find from $a^{(p-1)(i-j)k/q} = b^{(i-j)k} \equiv 1 (\mathrm{mod}\ p)$ that $p-1$ divides $(p-1)(i-j)k/q$, and so q divides $(i-j)k$, a contradiction.

Consider the product $\sigma' = \sigma \tau^{-b^k}$. Now, σ' fixes each point in P, but because of (13) it permutes the points of $P + t$ in a p-cycle. Unless $|S \cap (P + x)| \leq 1$ for every $x \in \{0, 1, ..., q-1\}$, we may also assume that $|S \cap P| \geq 2$. However, if $|S \cap P| \geq 2$, then σ' fixes S, implying that $(P + t) \subseteq S$, which is impossible.

We are left with the case that $|S \cap (P + x)| \leq 1$ for every $x \in \{0, 1, ..., q-1\}$. Note that, then the same holds for all lines $S + i$. It is obvious that $|S| \leq q$. Let $\{s\} = S \cap P$. As $\mathcal{C}$ is balanced, there are exactly $|S|$ lines through s. Now, each of the lines $S, S^{\sigma'}, ..., S^{\sigma'^{p-1}}$ contains s, while they intersect $P + t$ at distinct points. These imply in turn that, they are pairwise distinct, hence $|S| \geq p$, and so $p \leq |S| \leq q$, a contradiction. This completes the proof of case $v = pq$.

We turn next to the case $v = p^n$. Now, we cannot relay on a list of solving sets covering all cyclic objects as such list is available only when $v = p^2$ (see [9]). The argument below will be a combination of Lemma 4.4 with Sylow's theorems.

THE CASE $v = p^n$: Again, it is sufficient to consider connected configurations, the general case follows then by using the decomposition in (3) and induction on n. Let $\mathcal{C} = \mathrm{Con}(\mathbb{Z}_{p^n}, S)$ be a connected cyclic configuration, $G = \mathrm{Aut}(\mathcal{C})$ and C be the group generated by $\tau : x \mapsto x + 1$. Let G_p be a Sylow p-subgroup of G such that $C \leq G_p$. By Lemma 4.4 and Sylow's theorems it is sufficient to prove that $G_p = C$.

Towards a contradiction assume that $C < G_p$. Then the normalizer $N_{G_p}(C) > C$. Let us put $N = N_{G_p}(C)$ and let N_0 be the stabilizer of 0 in N. Then N_0 is non-trivial, and we may choose σ from N_0 of order p. Since σ normalizes the regular subgroup C and fixes 0, $\sigma = \mu_a$ for some $a \in \mathbb{Z}_{p^n}^*$ (see [5, Exercise 2.5.6]). Then $\mathrm{ord}_{\mathrm{m}}(a) = p$. Using the well-known structure of $\mathbb{Z}_{p^n}^*$ (cf. [10, Theorem 6.7 and Exercise 6.12]) we deduce that $n \geq 2$, and either

$$a = a'p^{n-1} + 1 \text{ for some } a' \in \{1, \ldots, p-1\},$$

or $n \geq 3$, $p = 2$ and $a \in \{2^n - 1, 2^{n-1} - 1\}$.

Assume for the moment that the latter case holds. Let $Q = \langle C, \sigma \rangle$. It is a routine exercise to show that C is the only cyclic subgroup of Q of order 2^n. This implies that the normalizer $N_{G_2}(Q) \leq N_{G_2}(C) = N$. Let H be an arbitrary regular cyclic subgroup of G. If $Q = G_2$, then, by Sylow's theorems, $H^g < Q$ for some $g \in G$, and so $H^g = C$, and we are done by Lemma 4.4. Thus we may assume that $Q < G_2$. Then $Q < N_{G_2}(Q) \leq N$. Choose an element $\sigma' \in N_0$ such that $\sigma' \neq \sigma$. It is well-known that $5^{2^{n-3}} \equiv 2^{n-1} + 1 (\mathrm{mod}\ 2^n)$ (see [10, Lemma 6.9]), and that $\mathbb{Z}_{2^n}^* = \langle 5 \rangle \times \langle -1 \rangle \cong \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$ (see [10, Theorem 6.10]). These imply that $\mu_{2^{n-1}+1} \in \langle \sigma, \sigma' \rangle$, and so $\mu_{2^{n-1}+1} \in N_0$. Therefore, we may assume that $\mu_a \in \mathrm{Aut}(\mathcal{C})$ where $a = a'p^{n-1} + 1$ for some $a' \in \{1, \ldots, p-1\}$.

Now, μ_a maps S to a line of $\mathcal{C}$, hence we may write $aS + b = S$ for some $b \in \mathbb{Z}_{p^n}$. Equivalently, S is a union of orbits of the affine transformation $\varphi : x \mapsto ax + b$. Then φ^p is equal to the translation $x \mapsto x + (1 + a + \cdots + a^{p-1})b$. By Corollary 2.3, S contains no non-trivial cosets. Form this and that S is a union orbits of φ^p, we find that $(1 + a + \cdots + a^{p-1})b \equiv 0 (\mathrm{mod}\ p^n)$. This quickly implies that p^{n-1} divides b, hence we may write $b = b'p^{n-1}$ for some $b' \in \{0, 1, ..., p-1\}$. Also,

$$\varphi : x \mapsto ax + b = x + (a'x + b')p^{n-1}.$$

From this we easily find the orbits of φ. For $x \in \mathbb{Z}_v$, let O be the orbit which contains x. Then

$$O = \begin{cases} \{x\} & \text{if } a'x + b' \equiv 0 (\mathrm{mod}\ p), \\ P + x & \text{otherwise,} \end{cases}$$

where $P = \{0, p^{n-1}, ..., (p-1)p^{n-1}\}$, i.e., the subgroup of $\mathbb{Z}_{p^n}$ of order p. Since X is connected, $\langle S - S \rangle = \mathbb{Z}_{p^n}$. This implies that $a's + b' \not\equiv 0 (\mathrm{mod}\ p)$ for some $s \in S$. But then the coset $(P + s) \subseteq S$, contradicting Corollary 2.3. The theorem is proved ∎

References

[1] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.

[2] S. Bays, Sur les systèmes cycliques des triples de Steiner différents pour N premier (ou puissance du nombre premier) de la forme $6n + 1$, *I. Comment. Math. Helv.* **2** (1930), 294–305.

[3] A. Betten, G. Brinkmann, and T. Pisanski, Counting symmetric configurations v_3, *Discrete Appl. Math.* **99** (2000), 331–338.

[4] M. Boben, T. Pisanski, A. Žitnik, I-graphs and the corresponding configurations, *J. Combin. Designs* **13** (2005), 406–424.

[5] J. D. Dixon, B. Mortimer, Permutation groups, Graduate Texts in Mathematics vol 163, Springer-Verlag, New York, 1996.

[6] B. Grünbaum, Configurations of points and lines, AMS, Graduate Studies in Mathematics vol. 103, 2009.

[7] M. Hladnik, D. Marušič, and T. Pisanski, Cyclic Haar graphs, *Discrete Math.* **244** (2002), 137–152.

[8] W. C. Huffman, The equivalence of two cyclic objects on pq elements, *Discrete Math.* **154** (1996), 103–127.

[9] W. C. Huffman, V. Job, V. Pless, Multipliers and generalized multipliers of cyclic objects and cyclic codes, *J. Combin. Theory Ser. A* **62** (1993), 183–215.

[10] G. A. Jones, J. M. Jones, Elementary number theory, Springer Undergraduate Mathematic Series, Springer-Verlag, London, 1998.

[11] D. Jungnickel, The isomorphism problem for abelian projective planes, *Applicable Algebra in Eng., Comm. and Comp.* **19**, (2008), 195–200.

[12] S. H. Koike-Quintanar, I. Kovács, Isomorphic tetravalent circulant Haar graphs, submitted to *Ars Math. Contemporanea* (preprint arXiv:1212.3208v1 [math. CO] (2012)).

[13] P. Lambossy, Sur une manière de différentcier les fonctions cycliques de 'une forme donnée, *I. Comment. Math. Helv.* **3** (1931), 69–102.

[14] M. Muzychuk, On the isomorphism problem for cycic combinatorial objects, *Discrete Math.* **197/198** (1999), 589–606.

[15] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, *Eur. J. Combin.* **8** (1987), 35–43.

[16] M. Petkovšek, T. Pisanski, Counting disconnected structures: chemical trees, fullerenes, I-graphs, and others, *Croat. Chem. Acta.* **78** (2005), 563–567.

[17] M. Petkovšek, H. Zakrajšek, Enumeration of I-graphs: Burnside does it again, *Ars Math. Contemp.* **2** (2009), 241262

[18] T. Pisanski, B. Servatius, Configurations from a graphical viewpoint, Birkhäuser, 2013.

[19] K. T. Phelps, Isomorphism problems for cyclic block designs, *Ann. Discrete Math.* **34** (1987), 385–392.

[20] D. Wiedemann and M. E. Zieve, Equivalence of sparse circulants: the bipartite Ádám problem, preprint arXiv:0706.1567v1 [math. CO] (2007).